数理解析研究所講究録
958 巻 1996 年 56-58

ON THE SOLUTIONS OF THUE EQUATIONS

MASAMI FUJIMORI (藤森雅己. 東北大理)

Let $k/\mathbb{Q}$ be a finite extension, $p(X,Y) \in k[X,Y]$ a homogeneous polynomial of degree $n > 3$ with non-zero discriminant, and $a \in k^\times = k \setminus \{0\}$. The equation

$$p(X,Y) = aZ^n$$

defines a regular curve C in $\mathbb{P}^2_k$ of genus $g = (n-1)(n-2)/2$.

Here we obtain an estimate for the number of integral solutions and a certain information about rational points.

Remark 0.1. In [2], we required that $p(X,Y)$ be divisible by a linear element in $k[X,Y]$, but it is easily seen we do not have to assume that. The same results follow if we replace the map f^a there by the map $f\colon C \to J =$ the Jacobian of C,

$$C(\bar{k}) \ni P \mapsto \mathcal{O}_C((2g-2)P - \text{a canonical divisor}) \in \operatorname{Pic}^0(C_{\bar{k}}) \simeq J(\bar{k})$$

which is defined over k, noting that this map equals $2g-2$ times f^a.

1. Integral solutions

For simplicity, we state the result only in the case of rational integral solutions. As for the algebraic S-integer version, we refer the reader to [2, Theorem 5.4].

In this section we assume that a and the coefficients of $p(X,Y)$ are in $\mathbb{Z}$.

In 1983, Silverman used the Jacobian variety J of C to estimate the number of integral solutions from above:

Theorem 1.1 (Silverman [4]). *If all the exponents of prime factors of a are less than n, and $|a|$ is sufficiently large, then*

$$\#\{(x,y) \in \mathbb{Z}^2 \mid p(x,y) = a\} < n^{2n^2}(8n^3)^R,$$

where $R = \operatorname{rank} J(\mathbb{Q})$.

1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G30.

We can think of $J(\mathbb{Q}) \otimes_{\mathbf{Z}} \mathbb{R}$ as a Euclidean space with some height function. He mapped $C(\mathbb{Q})$ to $J(\mathbb{Q})$ and counted the number of lattice points which lie in a ball of $J(\mathbb{Q}) \otimes_{\mathbf{Z}} \mathbb{R}$.

On the other hand, Mumford had asserted in 1965 paper [3] that in general, the heights of rational points on the Jacobian which come from a curve under a certain map increase at least exponentially if the genus is greater than 1.

Putting the above two results together, we obtain

Theorem 1.2. *If all the exponents of prime factors of a are less than n, and $|a|$ is sufficiently large, then*

$$\#\{(x,y) \in \mathbb{Z}^2 \mid p(x,y) = a\} \leq 4 \cdot 7^R,$$

where $R = \operatorname{rank} J(\mathbb{Q})$.

2. Rational points

For a general curve C over k of genus $g > 1$, there is a result of Vojta about the distribution of the rational points of C in the Jacobian variety J.

Let $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$ be respectively the inner product and the norm on $J(k) \otimes_{\mathbf{Z}} \mathbb{R}$ induced by the Néron-Tate height attached to the Θ-divisor.

Theorem 2.1 (Vojta [5], cf. [1]). *Assume $C(k) \neq \emptyset$. Regard $C \subset J$ by an appropriate map. For $\varepsilon > 0$, there exists a constant $\gamma = \gamma(C, \varepsilon)$ such that if $P, Q \in C(k)$ satisfy the inequalities $\|P\| > \gamma$ and $\|Q\| > \gamma \|P\|$, then*

$$\langle P, Q \rangle / \|P\| \|Q\| < 1/\sqrt{g} + \varepsilon.$$

If we have a non-trivial automorphism of the curve, what can we say about the distribution of the rational points of the curve? When asking this question, we prefer to use the morphism $f\colon C \to J$ given by

$$C(\bar{k}) \ni P \mapsto \mathcal{O}_C((2g-2)P - \text{a canonical divisor}) \in \operatorname{Pic}^0(C_{\bar{k}}) \simeq J(\bar{k}),$$

where $\bar{k}$ is an algebraic closure of k and $C_{\bar{k}} = C \times_k \operatorname{Spec} \bar{k}$. Automorphisms of C induce norm preserving morphisms of J compatible with the above map. In other words, there exists a canonically defined representation of $\operatorname{Aut}_k C$ on the Euclidean space $(J(k) \otimes_{\mathbf{Z}} \mathbb{R}, \| \cdot \|)$ which leaves the image of $C(k)$ stable.

In the case of Thue curves, we obtain the following result: Let C be the Thue curve as before. For an n-th root ζ of unity in k, we have an automorphism of C defined as

$$C(\bar{k}) \ni P = (x : y : z) \mapsto P_\zeta := (x : y : \zeta z) \in C(\bar{k}).$$

Proposition 2.2. *For $P \in C(k)$, if $\zeta \neq 1$ and $\|fP\| \neq 0$, then*

$$\langle fP_\zeta, fP\rangle / \|fP_\zeta\| \|fP\| = -1/(n-1).$$

As an application of this kind of results, if C is a twisted Fermat curve of degree 4, for example, we can see the rational points lie in an intersection of quadric hypersurfaces in $J(k) \otimes_{\mathbf{Z}} \mathbb{R}$. The author will explain it elsewhere.

References

1. E. Bombieri, The Mordell conjecture revisited, Ann. Scuola Norm. Sup. Pisa 17 (1990), 615–640; Errata-corrige, ibid. 18 (1991), 473.
2. M. Fujimori, On the solutions of Thue equations, Tôhoku Math. J. 46 (1994), 523–539.
3. D. Mumford, A remark on Mordell's conjecture, Amer. J. Math. 87 (1965), 1007–1016.
4. J.H. Silverman, Representations of integers by binary forms and the rank of the Mordell-Weil group, Invent. Math. 74 (1983), 281–292.
5. P. Vojta, Siegel's theorem in the compact case, Ann. of Math. 133 (1991), 509–548.

Mathematical Institute, Faculty of Science, Tohoku University, Sendai 980-77, Japan